75. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

B1

generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

receiving a second ciphertext from said remote party, sending g^x modulo p to said remote party, and starting a clock; receiving a third ciphertext and g^y modulo p from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

deriving a key k_B from g^y modulo p, computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, decrypting said second ciphertext with k_B to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

verifying that said second challenge signal is produced by said remote party;

producing a second response signal of minimum duration T, encrypting said second response signal with k_{AB} and sending a fourth ciphertext to said remote party;

verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with said remote party.

B1 cont.

76. The method according to claim 75, wherein said challenge signals and response signals represent biometrics characteristics (such as voice signals) of the producing parties.

77. The method according to claims 75, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

78. The method according to claim 75, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

B' Cont

79. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

means for receiving a second ciphertext from said remote party, sending g^x modulo p to said remote party, and starting a clock;

means for receiving a third ciphertext and g^y modulo p from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

means for deriving a key k_B from g^y modulo p, computing g^{xy}

modulo p, deriving a key k_{AB} from g^{xy} modulo p, decrypting said second ciphertext with k_B to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

means for verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

B1 Cont

means for verifying that said second challenge signal is produced by said remote party;

means for producing a second response signal of minimum duration T, encrypting said second response signal with k_{AB} and sending a fourth ciphertext to said remote party;

means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

80. The apparatus according to claim 79, wherein said challenge signals and response signals represent biometrics characteristics (such as voice signals) of the producing parties.

81. The apparatus according to claim 79, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

B/ cont

82. The apparatus according to claim 79, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

83. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

receiving a first ciphertext from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

receiving g^x modulo p from said remote party, deriving a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from said remote party;

verifying that said second challenge signal is produced by said remote party, producing a first response signal of minimum duration T;

B' Cont

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal, sending a third ciphertext and g^y modulo p to said remote party, and starting a clock;

receiving a fourth ciphertext, stopping the clock, and computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with the remote party.

84. The method according to claim 83, wherein said challenge signals and response signals represent biometrics characteristics (such as voice signals) of the producing parties.

85. The method according to claim 83, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

B1 Con't

86. The method according to claim 83, where TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the first challenge signal and t_4 being the duration of the second response signal.

87. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for receiving a first ciphertext from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

means for producing a first challenge signal of minimum duration T, where T is a fixed time interval and it is larger than the channel transmission and processing delay;

means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

B1
Cont

means for receiving g^x modulo p from said remote party, deriving a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from said remote party;

means for verifying that said second challenge signal is produced by said remote party, producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal, sending a third ciphertext and g^y modulo p to said remote party, and starting a clock;

means for receiving a fourth ciphertext, stopping the clock, and computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

B' Con't

means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

88. The apparatus according to claim 87, wherein said challenge signals and response signals are signals representing biometrics characteristics.

89. The apparatus according to claim 87, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

90. The apparatus according to claim 87, where TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the first challenge signal and t_4 being the duration of the second response signal.

B1 Cont

91. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

generating a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

generating a random number x, computing g^x modulo p, where g, and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

receiving g^y modulo p, computing a key k_B from g^y modulo p, decrytping the second ciphertext to recover a second challenge signal from said remote party;

verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

B1 Cont

receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with said remote party.

92. The method according to claim 91, wherein said challenge signals and response signals are signals representing biometrics characteristics.

93. The method according to claim 91, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

B1 Cont

94. The method according to claim 91, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said second response signal.

95. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

means for receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

means for receiving g^y modulo p, computing a key k_B from g^y modulo p, decrytping the second ciphertext to recover a second challenge signal from said remote party;

means for verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration T;

B1 cont

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

96. The apparatus according to claim 95, wherein said challenge signals and response signals are signals representing biometrics characteristics.

B1 Cont

97. The apparatus according to claim 95, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

98. The apparatus according to claim 95, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said second response signal.

99. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said method including the steps of:

receiving a first ciphertext from remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext;

B1 Cont

receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from remote party, sending g^y to remote party and starting a clock;

verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping the clock, decrypting said fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of the clock is within a predetermined interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with the remote party.

B1 Cont

100. The method according to claim 99, wherein said challenge signals and response signals are signals representing biometrics characteristics.

101. The method according to claim 99, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity of remote party's biometrics characteristics. Encryption of said challenge and response signals is performed using a cryptographic commitment function.

102. The method according to claim 99, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said first challenge signal and T_4 being the duration of said second

response signal.

103. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communication channel, said apparatus including:

means for receiving a first ciphertext from remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

B1 Cont

means for producing a first challenge signal of minimum duration T, where T is a fixed time interval, and it is larger than the channel transmission and processing delay;

means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext;

means for receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from remote party, sending g^y to remote party and starting a clock;

means for verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from

g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

means for receiving a fourth ciphertext from said remote party, stopping the clock, decrypting said fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of the clock is within a predetermined interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

104 The apparatus according to claim 103, wherein said challenge signals and response signals are signals representing biometrics characteristics.

105. The apparatus according to claim 103, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity of remote party's biometrics characteristics. Encryption of

said challenge and response signals is performed using a cryptographic commitment function.

B1 Con't

106. The method according to claim 103, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said first challenge signal and T_4 being the duration of said second response signal.

Respectfully submitted,

Julian H. Cohen
c/o Ladas & Parry
26 West 61st Street
New York, New York 10023
Reg. No. 20302
Tel. No. (212) 708-1887